
Froedtert Hospital

The Froedtert **HIPAA Privacy Officer** is Mary Wolbert. She can be reached at 414-805-2895.

The Froedtert & Community Health **HIPAA Security Officer** is Troy Schiesl. He can be reached at 414-777-5179.

You may also call the following with questions or concerns:

Compliance Offices: 414-805-2895
Compliance Hotline: 414-259-0220

REVISED NOVEMBER 2005

HIPAA Handbook



Froedtert Hospital

Dear Colleague:

As a health care provider in the community, Froedtert Hospital has been strongly committed to the privacy and confidentiality of health care information. Our patients rely on us to ensure that the record of the care and services they receive at Froedtert Hospital is kept confidential. In addition to this long standing commitment, the federal government recently passed a national rule regarding the privacy of health care information.

This handbook provides a brief overview of the Health Insurance Portability and Accountability Act (HIPAA) as it relates to our work. I recommend you review it thoroughly and keep it for easy reference. I also urge you to refer to the policies and procedures specified in this handbook for more detailed information as it relates to your job responsibilities. If you have questions about any of this information, please ask your supervisor or contact the resources listed on the back cover of this handbook.

Our continued success depends on each one of us maintaining the trust we have with our patients, providers of health care services, payers, research participants, and the community. By understanding the laws, regulations, and policies and procedures regarding patient privacy and by continuing to make sound decisions, we can continue to maintain our patients' trust.

Thank you for doing your part to uphold our world class reputation!

Sincerely,

William D. Petasnick
President and CEO

HIPAA including any of the following:

1. Using a unique health identifier
2. Obtaining identifiable health information
3. Disclosing identifiable health information

Fines:

- Up to \$50,000 and/or up to one year imprisonment

Offense: Knowingly misusing information under false pretenses

Fines:

- Up to \$100,000 and/or up to five years' imprisonment

Offense: Knowingly misusing information with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm

Fines:

- Up to \$250,000 and/or up to 10 years' imprisonment.

In Summary

Froedtert Hospital is committed to providing health care services consistent with the very highest standards of ethics and integrity. Each staff member, volunteer, student, business associate, and physician has a personal obligation to uphold our Organizational Code of Ethics. Complying with federal and state regulations is essential and demonstrates good business practices. The privacy and protection of our patients' confidential medical information demonstrates to patients and the community our commitment to their most basic rights and fosters a sense of trust. Without that trust, we cannot deliver the excellent patient-centered care to which we are dedicated.

HIPAA Security Officer

In addition, Froedtert has a designated **HIPAA Security Officer**. The security officer's role is to ensure the integrity of our information systems. As with privacy concerns and questions, you should speak with your supervisor or manager. If you are not comfortable doing this, contact the HIPAA Security Officer.

For any HIPAA privacy or HIPAA security issues, you may also contact the Corporate Compliance Office. Please be assured of your *absolute anonymity* in reporting any concern. At Froedtert, you can call the Corporate Compliance Hotline at (414) 259-0220.

HIPAA Penalties and Sanctions

Compliance with the HIPAA regulations is mandatory. The Office for Civil Rights is charged with enforcing any actions taken as a result of non-compliance. If a health care provider fails to implement the necessary steps to comply with the Privacy Regulations or if an individual or health care organization uses or discloses health information in a manner that is not allowed in the regulations, the penalties may include:

Civil Penalties:

Offense: General penalty for failure to comply with a Health Insurance Portability and Accountability Act of 1996 (HIPAA) provision:

Fines:

- Up to \$100 per person per violation
- Maximum of \$25,000 per person per year

Federal Penalties:

Offense: Penalty for a wrongful disclosure of individually identifiable health information knowingly and in violation of

What is HIPAA?

"HIPAA " stands for the **Health Insurance Portability and Accountability Act**. HIPAA was first introduced into Congress in 1996 and began as a bill addressing the portability of health care insurance. Its original goal was to ensure that those who had an employer-sponsored health insurance plan and changed jobs would not be denied health care benefits when they changed employers and their insurance plan. This meant it became necessary to transfer patient health care information from one insurance company to another and, many times, from one health care provider to another. Therefore, our governmental representatives have now created laws to ensure patients' health care information remains confidential. The law tells us how, when, and to whom we can share patients' health care information. The HIPAA privacy regulations were effective April 14, 2003.

Protected Health Information (PHI)

At the core of the HIPAA regulations is patient confidentiality of **Protected Health Information (PHI)**. PHI is any information, whether oral, written, electronic, magnetic, or recorded in any form, that:

- ✓ Is created or received by Froedtert Hospital as a health care provider,
 - ✓ Relates to an individual's past, present, or future:
 - physical or mental health condition
 - health care treatment
 - payment for health care services, and
 - ✓ Either clearly identifies an individual (i.e. name, social security number or medical record number) or can be used to find out the person's identity (address, telephone number, birth date, e-mail address, and names of relatives or employer).
-

Here are some examples of what is considered protected health information (PHI):

- ✓ *Name*
- ✓ *Address*
- ✓ *Employer*
- ✓ *Social security number*
- ✓ *Date of birth*
- ✓ *Telephone/fax number*
- ✓ *E-mail address*
- ✓ *Fingerprints or voiceprint*
- ✓ *Relatives' names*
- ✓ *Insurance information*
- ✓ *Medical record number*
- ✓ *Photos*
- ✓ *Other characteristics that may identify an individual*

Patient Rights:

HIPAA provides rights to patients as it relates to their PHI:

- ✓ The right to request access to their protected health information
- ✓ The right to request an amendment or correction to their protected health information
- ✓ The right to request the restriction or limit the use of their protected health information
- ✓ The right to refuse to be contacted for fundraising activities
- ✓ The right to keep their name off of the patient directory
- ✓ The right to receive a notice of hospital privacy practices

Protecting Protected Health Information

So, how do we protect PHI?

Individual Conduct

We are all personally responsible for respecting the privacy rights of our patients; this means not sharing patient information with anyone who should not have access to that

- PHI, Disposal of
- PHI, Requests for Communications by Alternative Means or Locations
- PHI, Right to Restrict Use and Disclosure of
- PHI, Security and Safeguarding of
- PHI, Use and Disclosure of
- Record Retention
- Solicitation of Funds and Receipt of Gifts

Fundraising and Marketing

HIPAA goes beyond clinical areas. The regulations affect how we conduct fund raising and marketing activities. Our Marketing Department is limited on how they communicate with patients. Patients also have a choice of whether to be contacted for fundraising.

Discarding PHI

The practice of Froedtert Hospital is to dispose of material containing protected health information into locked recycle bins. An outside vendor is utilized to destroy radiology films and jackets. Refer to the Disposal of PHI policy for details regarding disposal of tapes, CDs, diskettes, computer software, hardware, etc.

HIPAA Privacy Officer

Compliance with the HIPAA regulations is the responsibility of each and every staff member. If you have a concern or question related to confidentiality it is your personal responsibility to **report** this information to your immediate supervisor or other management staff. If you do not feel comfortable reporting your concern or asking a question of this person, Froedtert has a designated **HIPAA Privacy Officer** who is responsible for developing, coordinating, monitoring, and facilitating the hospital's compliance with federal and state laws that affect our information privacy practices. Any concerns from patients, visitors, volunteers, etc. should be forwarded to the Privacy Officer.

Examples of those who are required to sign Confidentiality Agreements are:

- ✓ Pharmaceutical sales representatives who may visit patient care settings and have incidental contact with PHI
- ✓ Any outside vendor that may come in contact with PHI but does not *require* PHI to conduct their business.

HIPAA Training

The HIPAA regulations require that all staff receive HIPAA education. In order to promote compliance with the HIPAA regulations and to ensure consistency in our interactions, the HIPAA privacy rules have been incorporated into Froedtert **Policies and Procedures**. Each department will review these Policies and Procedures to understand how they affect their departmental operations. Your management staff will provide further information and education regarding HIPAA.

Listed below are the policies and procedures affected by HIPAA. These are either newly written or received major revision as a result of the HIPAA regulations.

- Confidentiality
 - Education Programs, Mandatory/Required Attendance
 - Faxing of PHI
 - HIPAA Business Associate Agreements
 - HIPAA Joint Privacy Notice, Distribution of
 - Marketing Activities, Patient Confidentiality In
 - Patient Directory
 - Patient Rights and Responsibilities
 - Policy/Procedure Creation and/or Revision
 - PHI, Access and Disclosure to the Minimum Necessary Information
 - PHI, Access to by Patient or Patient Representative
 - PHI, Accounting for Disclosures of
 - PHI, Amendment of
 - PHI, Authorization Form for Uses and Disclosures of
 - PHI, De-Identification for Non-Research Purposes
-

information. We should not discuss our patients or their treatment in the cafeteria, in the elevator, with our friends outside of work, etc. We should pull curtains in patient rooms and close doors, if possible, in all areas of the hospital to protect our patients' privacy. Only those involved in the care and treatment of a patient are allowed access to that patient's medical record. These individuals include physicians, nurses, therapists, lab personnel, admitting staff, etc.

HIPAA refers to the types of services involved in the care of our patients as “**treatment, payment, or health care operations (TPO)**.” In other words, any staff who are involved in treatment of the patient, billing activities (payment) for those services, or other related health care operations, are allowed access to their confidential information. For example, communication of protected health information in the following circumstances is not restricted:

- ✓ Between various physicians taking care of the same patient
- ✓ Between any or all hospital employees involved in a patient's care
- ✓ To and from a patient's insurance company
- ✓ Quality assessment/improvement activities
- ✓ Care coordination/Case management
- ✓ Training, licensing, or other related activities

For some uses such as business planning or development, protected health information is de-identified so the information cannot be linked to any patient. De-identification means removing any information such as name, medical record number, or billing number, that would link this information to the patient.

Be aware that these requirements apply to *verbal, written, electronic, and magnetic* communications, or any other medium for maintaining information. This means we need to be mindful not only of our verbal or written communications but also of the risks associated with faxing or e-mailing healthcare information or leaving this information on answering machines.

Faxing

Written patient authorization is required for faxing any information other than for treatment, payment, or health care operations (TPO), or federal or state law or regulation. An approved hospital fax cover sheet must be used when sending protected health information via fax. All information must be completed on the sheet prior to faxing. Some extra precautions include having pre-programmed fax numbers. Prior to faxing, call the requester, verify the receiver's identity and fax number, and make sure they are available to receive the information before beginning transmission. The fax cover sheet asks the requestor to call and verify receipt of the faxed information. Please refer to the hospital policy on faxing of protected health information to review approved faxing protocols.

Interdepartmental Mail

All interdepartmental mail of a confidential nature is to be placed in a secured interoffice envelope and labeled, "Confidential," and is to be opened only by the addressee or designee. Original documentation and/or medical records should never be sent via inter-office mail.

E-mail

Protected health information should not be typed in the subject field of e-mail. If you are sending PHI via email to an external address, you should type 'secure' in the subject line to ensure that it gets encrypted. External email addresses do not include MCW.edu addresses. If you have any questions or concerns regarding Email security, please contact the Froedtert & Community Health Information Technology Security Officer.

Pneumatic Tube System

All protected health information transported via the pneumatic tube system must include whom the recipient is and the sender's name. Assume that all materials transported via the pneumatic tube system are confidential.

Authorizations are required for disclosure of protected health information for fundraising, certain marketing activities and research. If you have questions regarding authorizations, contact the Medical Records Department.

Business Associates

To further ensure that the privacy of our patients' PHI is protected, we have provided contracts to those companies with whom we do business. A **Business Associate (BA)** is a person or business, other than a member of the hospital's workforce, who performs services *on behalf of the hospital* or assists the hospital in normal operations, and who are involved in the use or disclosure of PHI. These Business Associates may have access to the confidential information of the hospital's patients in the course of performing their jobs. We have required our Business Associates to sign this agreement ensuring their compliance with the HIPAA regulations. Business Associate Agreements help to limit the use and disclosure of protected health information to the minimum amount necessary. Examples of Business Associates are:

- ✓ The vendor, whose staff provides Medical Records functions on behalf of the hospital
- ✓ Translation/interpretation companies who provide services on behalf of the hospital
- ✓ Computer software companies that may need to access our hospital computer systems to provide service/maintenance
- ✓ Temporary Agency Staff / Contracted Labor

The hospital may also do business with companies that do *not* perform a function *on behalf of the hospital* but who may come in contact with PHI in the course of their job responsibilities. These individuals or businesses are required to sign a Confidentiality Agreement stating that they understand and will comply with the HIPAA privacy rules and the rules of the hospital.

The minimum necessary standard also requires that we limit access to protected health information to those who truly need it to perform their job. For instance, a radiologic technologist may not need access to a patient's psychiatric consultation report in order to perform an x-ray of a patient's arm. Also, a nursing home may not need a copy of every progress note before a patient can be transferred to their facility.

Incidental Uses and Disclosures

An incidental use or disclosure is a disclosure of protected health information that cannot be reasonably prevented, is limited in nature, and occurs as a result of another use or disclosure of protected health information. For example, a customer overhears the pharmacist discussing a prescription with a patient over the pharmacy counter. Although incidental disclosures are allowable under HIPAA, you should make a reasonable effort to safeguard PHI.

Authorization

There are further protections under the Privacy Rule. Froedtert Hospital must have a valid **authorization** from an individual (or a person authorized by the individual) before we may **use or disclose** an individual's PHI for any purpose except to carry out treatment, payment, or health care operations or as permitted or required without authorization under federal and/or state law. Valid authorizations are specific to a particular disclosure, to a particular party, and for a particular reason. An authorization is not a blanket approval to release information. HIPAA provisions also mandate that authorizations:

- ✓ Must be in writing, signed and dated by the patient, and retained by the provider
- ✓ Are valid for one year from the date signed unless otherwise specified by the patient
- ✓ May be revoked in writing by the patient at any time
- ✓ May be signed by the patient's legal representative
- ✓ Are required in order to disclose PHI *to the patient*
- ✓ Must be tracked or accounted for by the provider
- ✓ Special authorization is required for disclosure of sensitive information including mental health, drug/alcohol treatment or HIV/AIDS

Electronics and PHI

Protected health information is not to be stored on local hard drives, laptops, portable media, devices such as Palm Pilots, and other devices without having the password protection/encryption required by the Froedtert & Community Information Technology Security Officer.

Overhead Paging

A patient's name should not be linked with a hospital service when overhead paging. It is acceptable to overhead page a patient to a phone extension.

Wireless Paging

Alpha pages should not contain a patient's name linked with any other identifiable information, including results, diagnosis, treatment information, etc.

Notice of Privacy Practices

HIPAA regulations require that we provide a written Notice of Privacy Practices to all patients and research participants. This document outlines their privacy rights, our responsibilities, and the policies and processes we have established to protect their privacy. The notice is posted in public areas of the hospital, is available in registration areas, and is available on our website at www.froedtert.com.

Minimum Necessary

Health care providers possess a lot of personal information about their patients. The HIPAA regulations use the term "**uses and disclosures**" to describe the acceptable communication or disclosure of patient information. The standard for disclosure of patient health care information incorporates an understanding of the "**minimum necessary.**" Complying with the minimum necessary standard means that we will make a reasonable effort to limit the amount of information we disclose; we are only to convey the minimum amount of protected health information necessary to accomplish the intended purpose of the communication.
